10/643 · 300 · 9-13-04

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/25928 A1

(51) International Patent Classification[7]: G06F 12/00, 9/00

(21) International Application Number: PCT/US00/26840

(22) International Filing Date:
29 September 2000 (29.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/157,472 1 October 1999 (01.10.1999) US
60/206,947 25 May 2000 (25.05.2000) US

(71) Applicant *(for all designated States except US)*: INFRAWORKS CORPORATION [US/US]; 504 Lavaca Street, Suite 1100, Austin, TX 78701 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FRIEDMAN, George [US/US]; 7109 Montana Norte, Austin, TX 78731 (US). STAREK, Robert, Phillip [US/US]; 3609 Del Robles, Austin, TX 78727 (US). MURDOCK, Carlos [US/US]; 4517 Avenue F, Austin, TX 78751 (US).

(74) Agents: TAUFER, Paul, A. et al.; Schnader Harrison Segal & Lewis, LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103-7286 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/25928 A1

(54) Title: METHOD AND APPARATUS FOR MONITORING CLOCK-RELATED PERMISSION ON A COMPUTER TO PREVENT UNAUTHORIZED ACCESS

(57) Abstract: To prevent unauthorized access on a computer, a clock monitoring system having a memory for storing a permission database having one or more permission fields, each field comprising one or more clock-related permissions, a time-value field comprising a stored time-value, and a clock-monitor in communication with the permission database. The clock-monitor reads a first time-value from a system clock, determines whether the permissions database is initialized, and if the permission database is initialized, compares the first time-value to the stored time-value. If the first time-value is later than the stored time-value, the clock-monitor stores the first time-value in the stored time-value field. If the first time-value is earlier than the stored time-value, the clock-monitor disables the one or more clock-related permissions, thereby preventing access to the data. If the permissions database is not initialized, the clock-monitor stores the first time-value in the stored time-value field.

Method and Apparatus for Monitoring Clock-Related Permission on a Computer to Prevent Unauthorized Access.

Field of the Invention

The invention relates to monitoring the system clock of a computer to detect alterations or modifications to the system clock. In particular, the invention relates to a method and apparatus for monitoring alterations or modifications of a system clock to prevent unauthorized access to secure data.

Background of the Invention

Some computer programs contain restrictions that limit the time of use of the program. These restriction may be either dictated by a license, agreed to conditions of use of a program, or defined by the owner or provider of the program. For example, trial versions of software typically permit use for a specified period, such as, for example, 30 days. One known method for setting the expiration period of the trial software is to record the system clock information, which includes date and time information, and set the expiration date to be the thirtieth day following that date. Another known method is to have the expiration date programmed into the computer code. Under this method, the program will operate only if the system clock date is earlier than the expiration date regardless of when the program is installed on the computer system.

According to either of these two methods, a user is prohibited from executing the computer program after the expiration date. Typically, an attempt to execute a program after expiration date generates a screen-message notifying the user that the program has expired. A known method to circumvent the expiration date parameter is to manually reset the system clock to a date and time that falls within the permitted time period, that is, to a time and date earlier than the expiration date.

Attempts have been made to address this problem by completely disabling a program independent of system clock information after a user tries to execute a program when the system clock date is later than the expiration field. However, this solution is harsh, in that it does not permit the user to correct the system clock and perhaps continue a permitted use of the software.

There is a need in the field of computer systems to prevent the circumvention of use-restrictions embedded in computer code, such as expiration parameters, without permanently disabling use or access to the program or data within it. The present invention addresses this need by providing a method and apparatus that monitors the system clock to prevent unauthorized access to data. The invention detects modifications or alterations to the system clock and disables clock-related permissions until the system clock is returned to its correct value.

Summary of the Invention

The invention relates to a clock monitoring system for monitoring alterations or

modifications of a system clock to prevent unauthorized access to secure data. One method of the invention comprises the steps of reading a first time value from the system clock and determining whether a permissions database, having one or more clock-related permission field, each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value, is initialized on the computer system. If so initialized, this method of the invention compares the first time value to the stored time value and, if the first time value is later than the stored time value, stores the first time value in the stored time value field, but if the first time value is earlier than the stored time value, disables the one or more clock-related permissions, whereby disabling the clock-related permissions prevents access to the data. If the permissions database is not initialized, the first time value is stored in the stored time value field.

Brief Description of the Drawings

For the purpose of illustrating the invention, there is shown in the drawings a form which is presently preferred; it being understood, however, that this invention is not limited to the precise arrangements and instrumentalities shown.

Figure 1 is a flow diagram of a method for monitoring alterations or modifications of a system clock according to an embodiment of the invention.

Figure 2 is a flow diagram of a method for monitoring alterations or modifications of a system clock by checking system clock values at predetermined tracking intervals.

Detailed Description of Preferred Embodiments of the Invention

The present invention comprises a novel method and apparatus for monitoring the system clock of a computer to prevent unauthorized access to data. The terms "computer", "computer system", or "system" as used herein include any device capable of receiving, transmitting, and/or using information, including, without limitation, a processor, a microprocessor, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. A computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system. Also, the terms "information" and "data" as used herein are each intended to include the broadest definition of the other. For example, the term "information" can mean raw data, processed data, or a combination of raw and processed data and includes but is not limited to text, audio and video data.

The following description is presented to enable any person skilled in the art to make and use

the invention. Descriptions of specific applications are provided only as examples. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiment shown. On the contrary, the description of the invention set forth herein is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

Referring now to Figure 1 there is shown a block diagram of a method for monitoring the system clock of a computer in accordance with a preferred embodiment of the present invention. According to this method, a clock monitor is in communication with a permissions database stored in a memory. The permissions database contains at least one clock-related permission field and a stored time value field having a stored time value. Each permission field contains at least one clock-related permission. The clock-related permissions are parameters which control access to data based on information from the system clock, such as time and date information, on the speed of the system clock. It is known in the art that computer systems operate substantially according to a system clock.

Clock-related permissions include, for example, specifying how long a user may access the data by date, hour or minute. One method of implementing this permission is to decrement the access time from the time a process accesses the data until the time the process expires. The access time is tracked internally; however, the speed of the system clock, denied from the ticks of the system processor, is used to decrement the access time. If, during the process, the access time is completely exhausted, the process would be automatically terminated. After the access time expires, the data would be overwritten and deleted. Another example of a clock-related permission is specifying a date on which the data will no longer be available. A user would have access to the data until the expiration date occurs. If a process has the data opened on the expiration date, the process would be automatically terminated and the data would be overwritten and deleted. Yet another example of a clock-related permission is specifying an authorization date on which the data will become accessible. According to this permission, a user would not be able to access the data until the authorization date has passed. Once the authorization date has passed, the user will have access to the data. Other examples of clock-related permissions include "no permissions" or "unrestricted use". The data subject to the clock-related permissions may be stored on a storage device, such as, for example, a hard disk, a floppy disk, a CD-ROM, or a magnetic tape, or may be embedded within the permissions database or computer program.

The clock monitor comprises computer code that, when executed, initiates the initialization of the clock monitor, step 12. In an embodiment of the invention, the computer code is a computer program stored on a machine-readable medium, such as, for example, a magnetic disk or an optical disk. The computer code may be a single module of code or, preferably, may be broken up into a series of modules for performing the functions of the clock monitor. In one embodiment, common

functions are performed more than once by a single module of code by issuing a call to perform the functions of the module of code. Upon initiation, the clock monitor reads the current time from the system clock, step 14. The clock monitor then determines whether the permissions database is initialized, which includes whether it has been initialized on a prior occasion, step 16. In one embodiment of the invention, the execution of a computer program causes the permissions database to initialize via a permission database driver. The database is considered "initialized" if the permissions database driver is loaded on the computer system. In this embodiment, the clock monitor computer code may be embedded within the computer program for initializing the permissions database. In another embodiment, the step of determining whether the permissions database is initialized involves reading the stored time value from the permissions database. If the stored time value is zero, then the database is not initialized. If the stored time value is other than zero, then the database is initialized.

If the permissions database is initialized, then the current time value from step 14 is compared to the stored time value in the stored time value field in the permissions database, step 18. If the current time value from step 14 is later than the stored time value, the current time value is stored in the stored time value field, step 20. If the current time value from step 14 is earlier than the stored time value, the clock-related permissions are disabled, thereby preventing access to the data, step 22.

If the permissions database is not initialized, the current time value of the system clock from step 14 is stored in the stored time value field, step 24. After either of steps 20, 22, or 24, the clock monitor is initialized, step 26, according to the method depicted in Figure 1.

Figure 2 shows a method according to one embodiment of the invention wherein, after the clock monitor is initialized, the system clock is checked at predetermined tracking intervals to verify the integrity of the system clock. The interval check is initiated in step 28. An internal clock increments the current time value from step 14 using the speed of the system clock and tracks a true system time. The true system time is the stored time value plus an internal elapsed time measured from the time the clock monitor was initialized. The internal elapsed time is preferably stored in the permissions database. At a predetermined tracking interval, the clock monitor reads the time value of the system clock, step 30, and compares it to the true system time kept by the internal clock, step 32. The predetermined tracking interval can be any time value but, preferably, is in the range of zero to sixty seconds. Most preferably, the predetermined tracking interval is one minute. Based on the comparison between the time value of the system clock, as read in step 30, and the true system time, the clock monitor generates a time deviation, also in step 32. The time deviation is compared against an acceptable deviation. The acceptable deviation is preferably predetermined and may be any value of time, such as, for example, a value of time within the range of zero seconds to three hours. Most preferably, the acceptable deviation is three hours.

If the time deviation is outside the acceptable deviation , the clock monitor concludes that

the system clock value has been altered and disables all clock-related permissions, step 34. If the time deviation is within the acceptable deviation, the clock monitor enforces the clock-related permissions, step 36. In step 38, the true system time is stored, preferably in the permissions database and the interval check is completed, step 40.

In one embodiment, the steps of Figure 2 are generally repeated if the clock-related permissions are disabled in step 34, or in step 22 of Figure 1. If the time deviation generated in this iteration of the steps in Figure 2 is within the acceptable deviation, the clock-related permissions are reenabled, permissions are enforced, as needed, the true system time is stored, preferably in the stored time value field of the permissions database, and the time value read from the system clock is stored in a last known good system field in the permissions database.

In another embodiment, when the computer shuts down, the true system time is compared to the system clock value. If the system clock value is within the accepted deviation, the system clock value is stored in the stored time value field. This enables relatively small deviations to be accounted for and stored.

What is claimed is:

1. A method of monitoring a system clock of a computer to prevent unauthorized access to data comprising the steps of:

initializing a clock monitor comprising the steps of:

reading a first time value from the system clock;

determining whether a permissions database having one or more clock-related permission field each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value, is initialized on the computer system;

if the permissions database is initialized, comparing the first time value to the stored time value and,

if the first time value is later than the stored time value, storing the first time value in the stored time value field,

if the first time value is earlier than the stored time value, disabling the one or more clock-related permissions, whereby disabling the clock-related permissions prevents access to the data; and

if the permissions database is not initialized, storing the first time value in the stored time value field.

2. The method of claim 1 wherein the step of determining whether the permissions database is initialized comprises the step of:

reading the stored time value from the stored time value field in the permissions database, and if the stored value is zero, concluding that the permissions database is not initialized, and if the stored time value field is other than zero, concluding that the permissions database is initialized.

3. The method of claim 1 further comprising the steps of:

tracking a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

after a predetermined tracking interval, reading a second time value from the system

clock;

comparing the second time value with the true system time and generating a time deviation based on the comparison;

if the time deviation is not within an acceptable deviation, disabling the one or more clock-related permissions;

if the time deviation is within the acceptable deviation, enforcing the clock-related permissions; and

storing the true system time.

4. The method of claim 3, after the step of if the time deviation is not within an acceptable deviation, disabling one or more clock-related permissions, further comprising the steps of:

reading a third time value from the system clock;
comparing the third time value with the true system time;
generating a second time deviation based on the comparison; and
if the second time deviation is within the acceptable deviation, reenabling the clock-related permissions, storing the true system time in the stored time value field, and storing the third time value in a last known good system time value field in the permissions database.

5. The method of claim 3 wherein the predetermined tracking interval is substantially in the range of zero seconds to sixty seconds.

6. The method of claim 3 wherein the accepted deviation is substantially in the range of zero seconds to three hours.

7. The method of claim 1 further comprising the steps of:

tracking a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

reading a second time value from the system clock;

comparing the second time value with the true system time and generating a time deviation based on the comparison; and

if the time deviation is within an acceptable deviation, storing the second time value in the stored time value field.

8. The method of claim 7 further comprising the step of powering down the computer.

9. The method of claim 7 wherein the accepted deviation is substantially in the range of zero seconds to three hours.

10. The method of claim 1 wherein the clock-related permissions comprise date-related permissions.

11. A clock monitoring system to prevent unauthorized access to data on a computer having a system clock, the system comprising:

a memory for storing a permissions database having one or more clock-related permission field each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value;

a clock monitor in communication with the permissions database that

reads a first time value from the system clock,

determines whether the permissions database is initialized,

if the permissions database is initialized, compares the first time value to the stored time value and,

if the first time value is later than the stored time value, stores the first time value in the stored time value field,

if the first time value is earlier than the stored time value, disables the one or more clock-related permissions, whereby disabling the clock-related permissions prevents access to the data; and

if the permissions database is not initialized, stores the first time value in the stored time value field.

12. The clock monitoring system of claim 11 wherein the clock monitor determines whether the permissions database is initialized by:

reading the stored time value from the stored time value field in the permissions database, and if the stored value is zero, concluding that the permissions database is not initialized, and if the stored time value field is other than zero, concluding that the permissions database is initialized.

13. The clock monitoring system of claim 11 wherein the clock monitor further:

tracks a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

after a predetermined tracking interval, reads a second time value from the system clock;

compares the second time value with the true system time and generates a time deviation based on the comparison; and

if the time deviation is not within an acceptable deviation, disables the one or more clock-related permissions;

if the time deviation is within the acceptable deviation, enforces the clock-related permissions; and

stores the true system time.

14. The clock monitoring system of claim 13 wherein the clock monitor, after disabling one or more clock-related permissions if the time deviation is not within an acceptable deviation:

reads a third time value from the system clock;
compares the third time value with the true system time;
generates a second time deviation based on the comparison; and
if the second time deviation is within the acceptable deviation, reenables the clock-related permissions, stores the true system time in the stored time value field, and stores the third time value in a last known good system time value field in the permissions database.

15. A machine-readable medium comprising secured data and a program to monitor a system clock of a computer to prevent unauthorized access to the secured data, the program comprising:

a memory for storing a permissions database having one or more clock-related permission field each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value;

means for reading a first time value from the system clock;

means in communication with the permissions database for determining whether the permissions database is initialized;

means for comparing the first time value to the stored time value if the permissions database is initialized;

means for storing the first time value in the stored time value field if the first time value is later than the stored time value,

means for disabling the one or more clock-related permissions if the first time value is earlier than the stored time value, whereby disabling the clock-related permissions prevents access to the data; and

means for storing the first time value in the stored time value field if the permissions database is not initialized.

16. The machine-readable medium of claim 15, wherein the means for determining whether the permissions database is initialized comprises:

means for reading the stored time value from the stored time value field in the permissions database; and

means for concluding that the permissions database is not initialized if the stored value is zero, and concluding that the permissions database is initialized if the stored time value field is other than zero.

17. The machine-readable medium of claim 15 wherein the program further comprises:

means for tracking a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

means for reading a second time value from the system clock after a predetermined tracking interval;

means for comparing the second time value with the true system time and generating a time deviation based on the comparison;

means for disabling the one or more clock-related permissions if the time deviation is not within an acceptable deviation;

means for enforcing the clock-related permissions if the time deviation is within the acceptable deviation; and

means for storing the true system time in a memory.

18. The machine-readable medium of claim 17 further comprising:

means for reenabling the clock-related permissions.

19. The machine-readable medium of claim 18 wherein the means for reenabling the clock-related permissions comprises:

means for reading a third time value from the system clock;
means for comparing the third time value with the true system time;
means for generating a second time deviation based on the comparison; and
means for storing the time system time in the stored time value field and storing the third time value in a last known good system time value field in the permission database if the second time deviation is within the acceptable deviation.

20. A method of monitoring a system clock to prevent unauthorized access to data comprising the steps of:

initializing a clock monitor comprising the steps of:
reading a first time value from the system clock;

determining whether a permissions database having one or more clock-related permission field each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value, is initialized on the computer system by:

reading the stored time value from the stored time value field in the permissions database, and if the stored value is zero, concluding that the permissions database is not initialized, and if the stored time value field is other than zero, concluding that the permissions database is initialized;

if the permissions database is initialized, comparing the first time value to the stored time value and,

if the first time value is later than the stored time value, storing the first time value in the stored time value field,

if the first time value is earlier than the stored time value, disabling the one or more clock-related permissions, whereby disabling the clock-related permissions prevents access to the data; and

if the permissions database is not initialized, storing the first time value in the stored time value field;

tracking a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

after a predetermined tracking interval, reading a second time value from the system clock;

comparing the second time value with the true system time and generating a time deviation based on the comparison; and

if the time deviation is not within an acceptable deviation, disabling the one or more clock-related permissions;

if the time deviation is within the acceptable deviation, enforcing the clock-related permissions;

storing the true system time;

if the clock-related permissions are disabled,

reading a third time value from the system clock;

comparing the third time value with the true system time;

generating a second time deviation based on the comparison; and

if the second time deviation is within the acceptable deviation, reenabling the clock-related permissions, storing the true system time in the stored time value field, and storing the third time value in a last known good system time value field in the permission database.

21. A machine-readable medium comprising secured data and a program to monitor a system clock of a computer to prevent unauthorized access to the secured data, the program comprising:

a memory for storing a permissions database having one or more clock-related permission field each field comprising one or more clock-related permissions, and a stored time value field comprising a stored time value;

a first module of computer code that reads a first time value from the system clock;

a second module of computer code that communicates with the permissions database to determine whether the permissions database is initialized;

a third module of computer code that compares the first time value to the stored time value if the permissions database is initialized and stores the first time value in the stored time value field if the permissions database is not initialized;

a fourth module of computer code that stores the first time value in the stored time value field if the third module compares the first time value to the stored time value and the first time value is later than the stored time value; and

a fifth module of computer code that disables the one or more clock-related permissions if the third module compares the first time value to the stored time value and the first time value is earlier than the stored time value, whereby disabling the clock-related permissions prevents access to the data.

22. The machine-readable medium of claim 21, wherein the second module of computer code comprises:

a sixth module of computer code for reading the stored time value from the stored

time value field in the permissions database; and

a seventh module of computer code for concluding that the permissions database is not initialized if the stored value is zero, and concluding that the permissions database is initialized if the stored time value field is other than zero.

23. The machine-readable medium of claim 21 wherein the program further comprises:

an eighth module of computer code that tracks a true system time, which is the stored time value plus an internal elapsed time measured from initialization of the clock monitor;

a ninth module of computer code that reads a second time value from the system clock after a predetermined tracking interval;

a tenth module of computer code that compares the second time value with the true system time and generates a time deviation based on the comparison; and

an eleventh module of computer code that disables the one or more clock-related permissions if the time deviation is not within an acceptable deviation;

a twelfth module of computer code that enforces the clock-related permissions if the time deviation is within the acceptable deviation; and

a thirteenth module of computer code that stores the true system time in a memory.

24. The machine-readable medium of claim 23 further comprising:

a fourteenth module of computer code that reenables the clock-related permissions.

25. The machine-readable medium of claim 24 wherein the fourteenth module of computer code comprises:

a fifteenth module of computer code that reads a third time value from the system clock;

a sixteenth module of computer code that compares the third time value with the true

system time;

a seventeenth module of computer code that generates a second time deviation based on the comparison; and

an eighteenth module of computer code that stores the true system time in the stored time value field and stores the third time value in a last known good system time value field in the permissions database if the second time deviation is within the acceptable deviation.

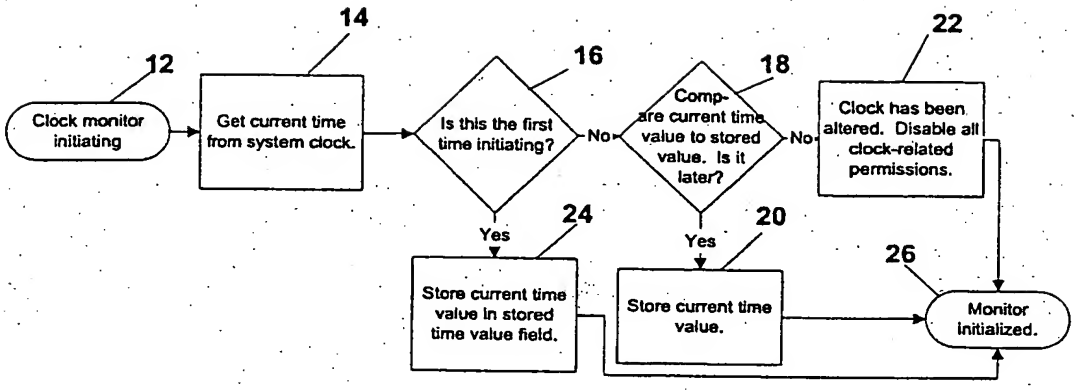

Fig. 1

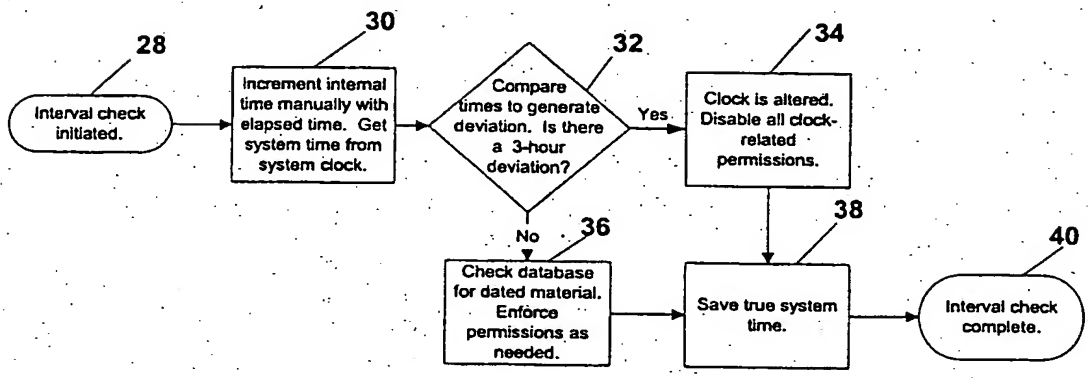

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/26840

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 12/00, 09/00
US CL : 711/163, 167; 713/502, 200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 711/163, 167; 713/502, 200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
WEST DATABASE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE Online

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,367,704 A (HASUO et al) 22 NOVEMBER 1994, Fig. 4, col. 1, lines 31-67, col. 3, lines 6-48.	1-2, 10-12, 15-16, 21-22
Y	US 5,761,651 A (hASEBE et al) 02 JUNE 1998, fig. 3, 4, 5, 13; col. 2, lines 3-16; col. 4, lines 23-52; col. 5, lines 18 to col. 6, line 41.	1-2, 10-12, 15-16, 21-22
A	US 5,343,524 A (MU et al) 30 AUGUST 1994, see the entire document.	1-25
A	US 5,014,234 A (EDWARDS, Jr.) 07 MAY 1991, see the entire document.	1-25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
02 NOVEMBER 2000

Date of mailing of the international search report
01 DEC 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
MATTHEW M. KIM James R. Matthews
Telephone No. (703) 305-0134

Form PCT/ISA/210 (second sheet) (July 1998)★